

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-305853

(43)Date of publication of application : 02.11.2000

(51)Int.Cl. G06F 12/14
// G09C 1/00

(21)Application number : 11-114661

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 22.04.1999

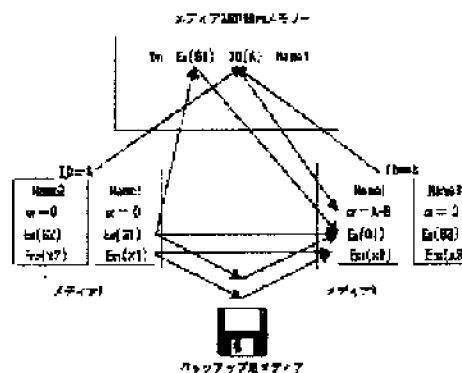
(72)Inventor : SUGAWARA TAKAYUKI
HIRATA ATSUMI

(54) METHOD FOR RECORDING CONTENTS INFORMATION AND CONTENTS INFORMATION PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to transfer a medium in which contents information is recorded between users while preventing the occurrence of illegal copying.

SOLUTION: In the case of transferring ciphered contents information EG1(x1) from a medium A to a medium B, cipher key information EA(G1) and the ID(A) of the medium A are recorded in a memory built in a medium controller as the management number Dn of data link ID. The number Dn is added to the information EG1(x1) and copied in the medium B together with the information EA(G1). The EA(G1) read out from the medium B is collated with the EA(G1) read out from the memory, and when the EA(G1) is matched with the EA(G1), a difference ID(A-B) value as a difference between the ID of the medium B and that of the medium A is outputted to the medium B. After outputting the difference ID(A-B) value, the EA(G1) and the ID(A) recorded in the memory are erased.



LEGAL STATUS

[Date of request for examination]

30.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-305853

(P 2 0 0 0 - 3 0 5 8 5 3 A)

(43) 公開日 平成12年11月2日(2000.11.2)

| (51) Int. Cl. ⁷ | 識別記号 | F I | キーワード (参考) | | |
|----------------------------|------|------------|------------|---|-------|
| G06F 12/14 | 320 | G06F 12/14 | 320 | E | 5B017 |
| | | | 320 | B | 5J104 |
| // G09C 1/00 | 660 | G09C 1/00 | 660 | G | |
| | | | 660 | D | |

審査請求 未請求 請求項の数15 O L (全18頁)

(21) 出願番号 特願平11-114661

(22) 出願日 平成11年4月22日(1999.4.22)

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者 菅原 隆幸

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(72) 発明者 平田 渥美

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 CA06
CA07 CA09 CA16

5J104 AA01 AA07 JA03 JA21 KA02

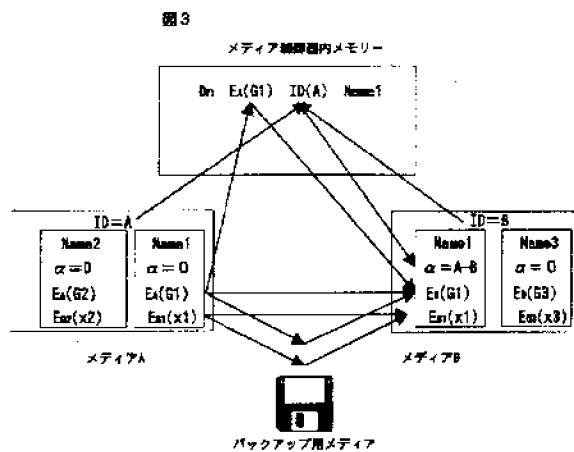
NA02 NA05 NA31 PA14

(54) 【発明の名称】 コンテンツ情報記録方法及びコンテンツ情報処理装置

(57) 【要約】

【課題】 不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡可能とする。

【解決手段】 メディアAからメディアBに暗号化コンテンツ情報EG1(X1)を譲渡する場合、暗号化鍵情報EA(G1)とメディアAのID(A)とはメディア制御器のメモリーにデータリンクIDの管理ナンバーDnとして記録される。EG1(X1)にはDnが付加されてEA(G1)と共にメディアBにコピーされる。メディアBから読み出したEA(G1)とメモリーから読み出したEA(G1)とを照合し一致している場合、メディアBとメディアAのIDの差分値である差分ID(A-B)値を、メディアBに出力する。出力後、メモリーに記録されているEA(G1)とID(A)を消去する。



【特許請求の範囲】

【請求項 1】 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録するコンテンツ情報記録方法であって、

前記第 1 のメディアのメディア ID に関する情報を前記第 1 及び第 2 のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第 2 のメディアに記録すると共に、前記第 1 のメディアから前記暗号化鍵情報を消去し、前記第 2 のメディアのメディア ID に関する情報と前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報とから形成される独自 ID 情報を前記第 2 のメディアに記録すると共に、前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報を消去することを特徴とするコンテンツ情報記録方法。

【請求項 2】 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録するコンテンツ情報記録方法であって、

前記第 1 のメディアのメディア ID に関する情報をデータリンク ID によって対応づけられた形態で前記第 1 及び第 2 のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とを前記第 2 のメディアに記録すると共に、前記第 1 のメディアから前記暗号化鍵情報を消去し、前記第 2 のメディアから読み出した前記データリンク ID を基に、前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報を得て、この第 1 のメディアのメディア ID に関する情報と前記第 2 のメディアのメディア ID に関する情報とから形成される独自 ID 情報を前記第 2 のメディアに記録すると共に、前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報を消去することを特徴とするコンテンツ情報記録方法。

【請求項 3】 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録するコンテンツ情報記録方法であって、前記第 1 のメディアのメディア ID に関する情報と前記

暗号化鍵情報とをデータリンク ID によって対応づけられた形態で前記第 1 及び第 2 のメディア以外の所定のメモリに一時記録し、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とを前記第 2 のメディアに記録すると共に、前記第 1 のメディアから前記暗号化鍵情報を消去し、

前記第 2 のメディアから読み出した前記データリンク ID を基に、前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを得、

前記第 2 のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その 2 つの暗号化鍵情報が一致しているときのみ、前記第 2 のメディアのメディア ID に関する情報と前記メモリから読み出した前記第 1 のメディアのメディア ID に関する情報とから形成される独自 ID 情報を前記第 2 のメディアに記録すると共に、前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを消去することを特徴とするコンテンツ情報記録方法。

【請求項 4】 前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報が、前記第 1 のメディアから読み出された第 1 のメディアのメディア ID に基づく情報であり、

前記第 2 のメディアのメディア ID に関する情報が、前記第 2 のメディアから読み出された第 2 のメディアのメディア ID に基づく情報であることを特徴とする請求項 1 ～ 3 のいずれか一つに記載のコンテンツ情報記録方法。

【請求項 5】 前記独自 ID 情報が、前記第 1 のメディアのメディア ID と前記第 2 のメディアのメディア ID との差分値である差分 ID 情報であることを特徴とする請求項 1 ～ 4 のいずれか一つに記載のコンテンツ情報記録方法。

【請求項 6】 前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記 ID 鍵は、第 1 のメディアのメディア ID を用いた共通鍵または第 1 のメディアのメディア ID を所定の関数により変換した情報を用いた共通鍵であることを特徴とする請求項 1 ～ 5 のいずれか一つに記載のコンテンツ情報記録方法。

【請求項 7】 第 1 のメディアのメディア ID に関する情報を一時記録するメモリと、

第 2 のメディアのメディア ID に関する情報と前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報とから独自 ID 情報を形成して、この独自 ID 情報を第 2 のメディアに記録する独自 ID 情報形成手段と、

前記独自 ID 情報形成後に前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報を消

去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項 8】前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報が、前記第 1 のメディアから読み出された第 1 のメディアのメディア ID に基づく情報であり、

前記第 2 のメディアのメディア ID に関する情報が、前記第 2 のメディアから読み出された第 2 のメディアのメディア ID に基づく情報であることを特徴とする請求項 7 に記載のコンテンツ情報処理装置。

【請求項 9】前記独自 ID 情報が、前記第 1 のメディアのメディア ID と前記第 2 のメディアのメディア ID との差分値である差分 ID 情報であることを特徴とする請求項 7 または 8 に記載のコンテンツ情報処理装置。

【請求項 1 0】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録する際の前記各メディアの ID に関する情報を処理するコンテンツ情報処理装置であって、

前記第 1 のメディアのメディア ID に関する情報を一時記録するメモリと、

前記第 2 のメディアのメディア ID に関する情報と前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報とから独自 ID 情報を形成して、前記暗号化コンテンツ情報と前記暗号化鍵情報とが前記第 2 のメディアに記録された後に、前記独自 ID 情報を前記第 2 のメディアに記録する独自 ID 情報形成手段と、前記独自 ID 情報形成後に前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項 1 1】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録する際の前記各メディアの ID に関する情報を処理するコンテンツ情報処理装置であって、

前記第 1 のメディアのメディア ID に関する情報をデータリンク ID によって対応づけられた形態で一時記録するメモリと、

前記データリンク ID を前記第 1 のメディアに記録するデータリンク ID 書き込み手段と、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とが前記第 2 のメディアに記録された後に、前記第 2 のメディアから読み出した前記データリン

ク ID を基に、前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報を得て、この第 1 のメディアのメディア ID に関する情報と前記第 2 のメディアのメディア ID に関する情報とから独自 ID 情報を形成して、前記独自 ID 情報を前記第 2 のメディアに記録する独自 ID 情報形成手段と、

前記独自 ID 情報形成後に前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項 1 2】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第 1 のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第 1 のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第 2 のメディアに記録する際の前記各メディアの ID に関する情報を処理するコンテンツ情報処理装置であって、

前記第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とをデータリンク ID によって対応づけられた形態で一時記録するメモリと、

前記データリンク ID を前記第 1 のメディアに記録するデータリンク ID 書き込み手段と、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とが前記第 2 のメディアに記録された後に、前記第 2 のメディアから読み出した前記データリンク ID を基に、前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを読み出すメモリ読み出し手段と、

前記第 2 のメディアから読み出した前記暗号化鍵情報と、前記メモリ読み出し手段により前記メモリから読み出した前記暗号化鍵情報とを照合する暗号化鍵情報照合手段と、

この暗号化鍵情報照合手段により前記 2 つの暗号化鍵情報が一致していると判断されたときのみ、前記第 2 のメディアのメディア ID に関する情報と前記メモリから読み出した第 1 のメディアのメディア ID に関する情報とから独自 ID 情報を形成して、前記独自 ID 情報を前記第 2 のメディアに記録する独自 ID 情報形成手段と、前記独自 ID 情報形成後に前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項 1 3】前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報が、前記第 1 のメディアから読み出された第 1 のメディアのメディア ID に基づく情報であり、

前記第 2 のメディアのメディア ID に関する情報が、前記第 2 のメディアから読み出された第 2 のメディアのメディア ID に基づく情報であることを特徴とする請求項

10～12のいずれか一つに記載のコンテンツ情報処理装置。

【請求項14】前記独自ID情報が、前記第1のメディアのメディアIDと前記第2のメディアのメディアIDとの差分値である差分ID情報であることを特徴とする請求項10～13のいずれか一つに記載のコンテンツ情報処理装置。

【請求項15】前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ID鍵は、第1のメディアのメディアIDを用いた共通鍵または第1のメディアのメディアIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とする請求項10～14のいずれか一つに記載のコンテンツ情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、これに使用したコンテンツ鍵に対してそのメディアのIDをID鍵として暗号化した暗号化鍵情報とを、記録再生するコンテンツ情報暗号化システムに関するものである。そして、この発明はコンテンツ情報（特にオーディオやビデオのデータ）を配信し、配信されたデータを不正なコピーを阻止しながら、ユーザーのメディア間でのデータの譲渡（移動）を安全に行うことのできるコンテンツ情報暗号化システムにおけるコンテンツ情報記録方法及びコンテンツ情報処理装置を提供することを目的としている。

【0002】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのデジタルデータを配信する有用な方法として、特開平10-269289号公報に記載のデジタルコンテンツ配布管理方法、デジタルコンテンツ再生方法及び装置がある。この発明においては、デジタルコンテンツの配布側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツの使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。また、特開平9-25303号公報に記載の情報記録媒体、記録装置、情報伝送システム、暗号解読装置がある。この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の

条件情報が記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザー側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止した。

【0003】

【発明が解決しようとする課題】しかしながら上記の従来の方式では、コンテンツデータの記録されたメディアを、ユーザー間で譲渡することが出来ない（メディア自体の譲渡はできてもそのメディアに記録されたコンテンツデータの正規の再生ができない。）ので、ユーザーがコンテンツデータを手に入れるためには、一度は必ず課金管理機関、データ管理センター等に接続しなければならない。また、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメディアにデータを復帰させることができない。本発明は、コンテンツ情報を配信し、配信されたデータを不正なコピーを阻止しながら、ユーザーのメディア間でのデータの譲渡（移動）を安全に行うことのできるコンテンツ情報暗号化システムにおけるコンテンツ情報記録方法及びコンテンツ情報処理装置を提供することを目的としている。

【0004】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記の方法、装置を提供するものである。

（1）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録するコンテンツ情報記録方法であって、前記第1のメディアのメディアIDに関する情報を前記第1及び第2のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第2のメディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、前記第2のメディアのメディアIDに関する情報と前記メモリに一時記録された第1のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録すると共に、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去することを特徴とするコンテンツ情報記録方法。

（2）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録するコ

ンテンツ情報記録方法であって、前記第1のメディアのメディアIDに関する情報をデータリンクIDによって対応づけられた形態で前記第1及び第2のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとを前記第2のメディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、前記第2のメディアから読み出した前記データリンクIDを基に、前記メモリに一時記録された第1のメディアのメディアIDに関する情報を得て、この第1のメディアのメディアIDに関する情報と前記第2のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録すると共に、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去することを特徴とするコンテンツ情報記録方法。

(3) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録するコンテンツ情報記録方法であって、前記第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とをデータリンクIDによって対応づけられた形態で前記第1及び第2のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとを前記第2のメディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、前記第2のメディアから読み出した前記データリンクIDを基に、前記メモリに一時記録された第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とを得、前記第2のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その2つの暗号化鍵情報が一致しているときのみ、前記第2のメディアのメディアIDに関する情報と前記メモリから読み出した前記第1のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録すると共に、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とを消去することを特徴とするコンテンツ情報記録方法。

(4) 前記メモリに一時記録された第1のメディアのメディアIDに関する情報が、前記第1のメディアから読み出された第1のメディアのメディアIDに基づく情報であり、前記第2のメディアのメディアIDに関する情報が、前記第2のメディアから読み出された第2のメディアのメディアIDに基づく情報であることを特徴とする上記(1)～(3)のいずれか一つに記載のコンテンツ情報記録方法。

(5) 前記独自ID情報が、前記第1のメディアのメデ

ィアIDと前記第2のメディアのメディアIDとの差分値である差分ID情報であることを特徴とする上記

(1)～(4)のいずれか一つに記載のコンテンツ情報記録方法。

(6) 前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ID鍵は、第1のメディアのメディアIDを用いた共通鍵または第1のメディアのメディアIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とする上記(1)～(5)のいずれか一つに記載のコンテンツ情報記録方法。

(7) 第1のメディアのメディアIDに関する情報を一時記録するメモリと、第2のメディアのメディアIDに関する情報と前記メモリに一時記録された第1のメディアのメディアIDに関する情報とから独自ID情報を形成して、この独自ID情報を第2のメディアに記録する独自ID情報形成手段と、前記独自ID情報形成後に前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

(8) 前記メモリに一時記録された第1のメディアのメディアIDに関する情報が、前記第1のメディアから読み出された第1のメディアのメディアIDに基づく情報であり、前記第2のメディアのメディアIDに関する情報が、前記第2のメディアから読み出された第2のメディアのメディアIDに基づく情報であることを特徴とする上記(7)に記載のコンテンツ情報処理装置。

(9) 前記独自ID情報が、前記第1のメディアのメディアIDと前記第2のメディアのメディアIDとの差分値である差分ID情報であることを特徴とする上記

(7)または(8)に記載のコンテンツ情報処理装置。

(10) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する際の前記各メディアのIDに関する情報を処理するコンテンツ情報処理装置であって、前記第1のメディアのメディアIDに関する情報を一時記録するメモリと、前記第2のメディアのメディアIDに関する情報と前記メモリに一時記録された第1のメディアのメディアIDに関する情報とから独自ID情報を形成して、前記暗号化コンテンツ情報と前記暗号化鍵情報とが前記第2のメディアに記録された後に、前記独自ID情報を前記第2のメディアに記録する独自ID情報形成手段と、前記独自ID情報形成後に前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

(11) 所定のコンテンツ鍵で暗号化された暗号化コン

テンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する際の前記各メディアのIDに関する情報を処理するコンテンツ情報処理装置であって、前記第1のメディアのメディアIDに関する情報をデータリンクIDによって対応づけられた形態で一時記録するメモリと、前記データリンクIDを前記第1のメディアに記録するデータリンクID書き込み手段と、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとが前記第2のメディアに記録された後に、前記第2のメディアから読み出した前記データリンクIDを基に、前記メモリに一時記録された第1のメディアのメディアIDに関する情報を得て、この第1のメディアのメディアIDに関する情報と前記第2のメディアのメディアIDに関する情報とから独自ID情報を形成して、前記独自ID情報を前記第2のメディアに記録する独自ID情報形成手段と、前記独自ID情報形成後に前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

(12) 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する際の前記各メディアのIDに関する情報を処理するコンテンツ情報処理装置であって、前記第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とをデータリンクIDによって対応づけられた形態で一時記録するメモリと、前記データリンクIDを前記第1のメディアに記録するデータリンクID書き込み手段と、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとが前記第2のメディアに記録された後に、前記第2のメディアから読み出した前記データリンクIDを基に、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とを読み出すメモリ読み出し手段と、前記第2のメディアから読み出した前記暗号化鍵情報と、前記メモリ読み出し手段により前記メモリから読み出した前記暗号化鍵情報とを照合する暗号化鍵情報照合手段と、この暗号化鍵情報照合手段により前記2つの暗号化鍵情報が一致していると判断されたときのみ、前記第2のメディアのメディアIDに関する情報と前記メモリから読み出した第1のメディアのメディアIDに関する情報とから独自ID情報を形成して、前記独自ID情報を前記第2のメディアに記録する独自ID情報形成手段と、前記独自ID情報

形成後に前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とを消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

(13) 前記メモリに一時記録された第1のメディアのメディアIDに関する情報が、前記第1のメディアから読み出された第1のメディアのメディアIDに基づく情報であり、前記第2のメディアのメディアIDに関する情報が、前記第2のメディアから読み出された第2のメディアのメディアIDに基づく情報であることを特徴とする上記(10)～(12)のいずれか一つに記載のコンテンツ情報処理装置。

(14) 前記独自ID情報が、前記第1のメディアのメディアIDと前記第2のメディアのメディアIDとの差分値である差分ID情報であることを特徴とする上記(10)～(13)のいずれか一つに記載のコンテンツ情報処理装置。

(15) 前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ID鍵は、第1のメディアのメディアIDを用いた共通鍵または第1のメディアのメディアIDを所定の関数により変換した情報を用いた共通鍵であることを特徴とする上記(10)～(14)のいずれか一つに記載のコンテンツ情報処理装置。

【0005】

【発明の実施の形態】本発明によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、本発明によれば、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメディアにデータを復帰させるシステムを提供できる。

【0006】本発明では、

[a] 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録するコンテンツ情報記録する場合に、前記第1のメディアのメディアIDに関する情報を前記第1及び第2のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第2のメディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、前記第2のメディアのメディアIDに関する情報と前記メモリに一時記録された第1のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録すると共に、前記メモ

記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する場合に、前記第1のメディアのメディアIDに関する情報を前記第1及び第2のメディア以外の所定のメモリに一時記録して、前記第1のメディアから前記暗号化コンテンツ情報と前記暗号化鍵情報とをバックアップ用メディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第2のメディアに記録すると共に、前記第2のメディアのメディアIDに関する情報と前記メモリに一時記録された第1のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録し、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去するようにした。

[e] 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する場合に、前記第1のメディアのメディアIDに関する情報をデータリンクIDによって対応づけられた形態で前記第1及び第2のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとをバックアップ用メディアに記録すると共に、前記第1のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクIDとを前記第2のメディアに記録すると共に、前記第2のメディアから読み出した前記データリンクIDを基に、前記メモリに一時記録された第1のメディアのメディアIDに関する情報を得て、この第1のメディアのメディアIDに関する情報と前記第2のメディアのメディアIDに関する情報とから形成される独自ID情報を前記第2のメディアに記録すると共に、前記メモリから前記一時記録された第1のメディアのメディアIDに関する情報を消去するようにした。

〔f〕所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第1のメディアのメディアIDに関する情報をID鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第1のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第2のメディアに記録する場合に、前記第1のメディアのメディアIDに関する情報と前記暗号化鍵情報とをデータリンクIDによって対応づけられた形態で前記第1及び第2のメディア以外の所

50

定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とをバックアップ用メディアに記録すると共に、前記第 1 のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンク ID とを前記第 2 のメディアに記録すると共に、前記第 2 のメディアから読み出した前記データリンク ID を基に、前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを得、前記第 2 のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その 2 つの暗号化鍵情報が一致しているときのみ、前記第 2 のメディアのメディア ID に関する情報と前記メモリから読み出した前記第 1 のメディアのメディア ID に関する情報とから形成される独自 ID 情報を前記第 2 のメディアに記録すると共に、前記メモリから前記一時記録された第 1 のメディアのメディア ID に関する情報と前記暗号化鍵情報とを消去するようにした。

【0008】[g] 前記メモリに一時記録された第 1 のメディアのメディア ID に関する情報が、前記第 1 のメディアから読み出された第 1 のメディアのメディア ID に基づく情報であり、前記第 2 のメディアのメディア ID に関する情報が、前記第 2 のメディアから読み出された第 2 のメディアのメディア ID に基づく情報であるようにした。

[h] 前記独自 ID 情報が、前記第 1 のメディアのメディア ID と前記第 2 のメディアのメディア ID との差分値である差分 ID 情報であるようにした。

[i] 前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記 ID 鍵は、第 1 のメディアのメディア ID を用いた共通鍵または第 1 のメディアのメディア ID を所定の関数により変換した情報を用いた共通鍵であるようにした。

【0009】[j] 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、他のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報と、前記他のメディアのメディア ID に関する情報と本メディアのメディア ID に関する情報とから形成された独自 ID 情報とが記録されたメディアからコンテンツ情報を復元する場合に、前記独自 ID 情報と前記本メディアのメディア ID とから前記他のメディアのメディア ID に関する情報とを得て、前記暗号化鍵情報から前記コンテンツ鍵を復元し、このコンテンツ鍵を用いて前記暗号化コンテンツ情報を復元するようにした。

[k] 所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、他のメディアのメディア ID に関する情報を ID 鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報と、前記他のメディアのメディア ID に関する情報

と本メディアのメディア ID に関する情報とから形成された独自 ID 情報とが記録されているメディアとした。

[l] 前記独自 ID 情報を形成するための前記他のメディアのメディア ID に関する情報は、前記他のメディアから読み出したそのメディアのメディア ID に基づく情報であり、前記独自 ID 情報を形成するための前記本メディアのメディア ID に関する情報は、前記本メディアから読み出したそのメディアのメディア ID に基づく情報であるようにした。

[m] 前記独自 ID 情報が、前記他のメディアのメディア ID と前記本メディアのメディア ID との差分値である差分 ID 情報であるようにした。

[n] 前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記 ID 鍵は、前記他のメディアのメディア ID を用いた共通鍵または前記他のメディアのメディア ID を所定の関数により変換した情報を用いた共通鍵であるようにした。

【0010】まず、図 2 を用いて本発明の一実施例の構成を説明する。メディアはメディア固有の ID が設定され、メディア制御器にセットすることが出来る。メディアは記録再生可能であり、固有の ID を設定可能なものであれば、固体メモリーやディスク、テープ等でも良い。但し、ID 情報が所定の耐タンパー性をもつことが条件である。即ち、ID や暗号化に必要な鍵の保管に対して不正に情報を読み出したり、書き換えたりするのが難しい状態になっていることが望ましい。

【0011】もっとも簡単なものはメモリータイプでこのメモリーカードは所定のメモリー制御器を介してし、ID や暗号化鍵情報が引き出せない仕組みになっているものが、安全で簡単に作成できる。メモリーカードは、工場生産時にカード毎に固有な ID が記録されている。もしくは発行装置により発行される際に、そのメモリー固有の ID を EEPROM など記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにする。メディアには一部のデータのみメディア間のコピーを行うことの出来るメディアバスを有している。

【0012】メディア制御器はメディアをセットして、PC もしくは専用器などの端末に接続し、メディア内のデータと、端末とのインターフェース機能と、所定の ID でのデータの暗号化、復号化機能を有する。メディア制御器は端末側からメモリーの内部を不正にアクセスできない耐タンパー性をもっている。端末は外部にあるコンテンツ情報を配信をするセンター（配信センター）に接続し、課金、認証など所定の手続きを経て、コンテンツデータを受信する。センターとの接続はインターネットなどのネットワークはもちろん、ISDN や放送、ケーブル TV、PHS などの無線接続でもかまわない。

【0013】コンテンツ情報は基本的にコンテンツ毎に

違う鍵（コンテンツ鍵）で暗号化される。コンテンツは MPEG などの所定の圧縮方式によって圧縮された後、DES などの暗号化がなされている。例えば DES の場合、暗号化鍵は 64 ビット程度である。データベースとセンターと端末の関係を図 1 に示す。センターに設置したデータベースで、コンテンツ情報が、コンテンツ X1 を暗号化鍵 G1 で暗号化し、また、違うコンテンツ X2 を暗号化鍵 G2 で暗号化するものとして管理されている。

【0014】このセンターには複数の端末がネットワークで接続されている。端末への送信もセキュリティーを考慮して公開鍵方式で暗号化して送信する。ここで端末 1 (T1) の公開鍵を T1P とし、復号鍵を T1D とすると、データベース 1 に管理されていたコンテンツ X1 は、暗号化鍵 G1 で暗号化され E G1 (X1) という暗号化コンテンツ情報とされる。暗号化鍵 G1 は、端末 T1 に送信するために端末 T1 の公開鍵 T1P を使用して暗号化され、暗号化鍵の情報 E T1P (G1) となる。そして、暗号化コンテンツ情報 E G1 (X1) と暗号化鍵の情報 E T1P (G1) との 2 つの情報を端末 1 (T1) に送信する。

【0015】端末 1 でこのコンテンツ情報を再生するためには、端末 1 の復号鍵 T1D を用いて、暗号化鍵の情報 E T1P (G1) を復号し、暗号化鍵 G1 を得て、その暗号化鍵 G1 で暗号化コンテンツ情報 E G1 (X1) を復号し、コンテンツ X1 を得て、MPEG などの復号を行うことで再生することが出来るが、ここでは、送信されたデータを端末で再生することなく、すぐに端末に接続されたメディアに記録することを前提とする。ここでは公開鍵を使って端末までのデータ送信を説明したが、これは、共通鍵方式であっても、また他の方式であっても本発明はサポートすることが出来る。

【0016】次に図 3、4、5 を用いて本発明の一実施例のコンテンツ情報と鍵情報の受け渡し機能について説明する。

【0017】最初に配信センターから端末 T1 側のメディア A (第 1 のメディア) にコンテンツデータを受信する場合を説明する。まず、メディア A をメディア制御器にセットする。メディア制御器を端末 T1 にセットして、「データ記録モード」にする。課金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵 G1 で暗号化されて端末に配

信されてくる。
【0018】即ち、コンテンツ X1 を暗号化鍵 G1 で暗号化した暗号化コンテンツ情報 E G1 (X1) が送信されてくる。また、暗号化鍵 G1 を端末 T1 に送信するために、端末 T1 の公開鍵 T1P を使用して暗号化鍵 G1 を暗号化した暗号化鍵情報 E T1P (G1) が端末 T1 に送信されてくる。端末で復号に使用する鍵は T1D なので、この暗号化鍵情報 E T1P (G1) は復号鍵 T1D で復号できる。この状態を E T1D (G1) と表現する。端末ではこの暗号化鍵情報 E T1D (G1) を一度復号鍵 T1D で復号して暗号化鍵 G1 を得る。

【0019】メディア制御器ではこのデータを受信し、メディア A には暗号化コンテンツ情報 E G1 (X1) が記録され、同時にメディア制御器はセットされたメディアの ID を認識して、この鍵 G1 をメディア A の固有の ID である A という値で再暗号化して暗号化鍵情報 E A (G1) を得、これをメディア A に記録する。この時点でのメディア A の内容を図 3 のメディア A のブロックに示す。α は後述する差分 ID (独自 ID 情報) であり、この時点では α = 0 が記録されている。配信直後のデータ構造を図 4 (1) に示す。データは先頭に差分 ID 64 ビット、暗号化鍵情報 64 ビット、その後ろに暗号化コンテンツ情報が記録される。

【0020】次に、メディア A に記録されている暗号化コンテンツ情報を再生する場合を説明する。メディア A をメディア制御器にセットし、メディア制御器を「データ再生モード」とする。暗号化鍵情報 E A (G1) を自分の ID である A に α を加算した値を用いて暗号化鍵 G1 を復号し、次に暗号化鍵 G1 を用いて暗号化コンテンツ情報 E G1 (X) を復号して再生データ X を得ることが出来る。ここでは α = 0 なので ID = A を用いて復号した場合と等価である。

【0021】次に、メディア A (第 1 のメディア) からメディア B (第 2 のメディア) へデータを譲渡 (移動) する場合を説明する。コンテンツの記録されている譲渡元メディア A から譲渡先メディア B に暗号化コンテンツ情報を譲渡する場合、まず、メディア制御器にメディア A をセットする。メディア制御器のモードを「データ移動モード」にする。

【0022】暗号化鍵情報 E A (G1) と譲渡元メディア A (第 1 のメディア) の ID はメディア制御器のメモリーにデータリンク ID によって対応づけられた形態で一時的に記録される。これは図 3 のメディア制御器内メモリーのブロックに示したように、データリンク ID として Dn という管理ナンバーを一つ選ぶ。これは 0 から始めて 64 ビット以内であれば、シリアルに ID をつけて行くような形態でかまわない。後述するような、データリンク ID を消去する場合に、矛盾なく管理できればどのような打ち方でもかまわない。Dn に関連して、暗号化鍵情報 E A (G1) とメディア A の ID、及びコンテンツのネームなどが記録される。メディア A には複数のコンテンツが記録される場合も考慮してファノールネーム等、この Dn に関連してデータを記録する。

【0023】暗号化コンテンツ情報 E G1 (X1) には上記データリンク ID が付加されて、暗号化鍵情報 E A (G1) と共に、譲渡先メディアにコピーされる。暗号化コンテンツ情報、暗号化鍵情報 E A (G1) はメディアバスを介して高速にメディア B に転送される。このメディアバスは、メディア A とメディア B を物理的に連結して、メディア制御器を介さずにデータ転送を行うものである。このデータ自体は暗号化コンテンツデータのみがこのメディアバス

を通過できるようになっているので安全性が高い。暗号化コンテンツ情報構造を図4(2)に示す。メディアAからメディアBに暗号化コンテンツ情報EG1(X1)と暗号化鍵情報EA(G1)とを送信した後、譲渡元のメディアAにある暗号化鍵情報EA(G1)は消去される。また、セキュリティを考えると暗号化コンテンツ情報EG1(X1)も消去することが望ましいが暗号化鍵情報EA(G1)だけ消去されれば、それで暗号の復号はほぼ不可能と考えられる。

【0024】メディア内部、及びメディア制御器は、外部のバックアップ用メディアや、PCなどの端末などのように外部からの不正なアクセスをすることが不可能であり、情報の消去などのコマンドも確実に実行される。

【0025】次に、メディア制御器にメディアBをセットする。メディア制御器では、接続された譲渡先メディアBのIDを読み取り、次に、すでに転送されている暗号化コンテンツ情報EG1(X1)に付加されたデータリンクIDのDnを読み取る。また、暗号化鍵情報EA(G1)も同時に読み取る。メディア制御器この時点で「データ移動モード」であるので、差分IDと同じエリアに記録されたデータをデータリンクIDのDnとして認識できる。それをもとにメディア制御器のメモリーからデータリンクIDのDnに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのIDであるID(A)を読み取る。

【0026】ここで、譲渡先メディアBから読み出したEA(G1)と制御器メモリーから読み出したEA(G1)とを照合する。この鍵情報が一致していなければ以下のプロセスである差分IDを発行しない。即ち、一致していなかった場合、データリンクIDが同じでも違ったコンテンツの情報として認識することが出来る。これは、同一のメディアAから複数のメディア制御器を使って、データ移動を行った場合に発生する問題を回避するため、また、不正にコピーしようとしてメディア制御器内メモリーのデータや、メディア内データを改竄しようとした場合に発生する矛盾を発見し、機能を停止するのに効果を発揮する。

【0027】次に、認証の結果一致している場合、譲渡先メディアBと譲渡元メディアAのIDの差分値である差分ID、(A-B)値を、譲渡先メディアBに記録する。そして記録後、メディア制御器のメモリーに記録されている前記暗号化鍵情報EA(G1)と譲渡元メディアAのID(A)を消去する。この時点でのメディアBの内容を図3のメディアBのブロックに示す。

【0028】この消去の動作はメディア間でデータをコピーするのではなく、譲渡(移動)することを可能としている。もともとIDを用いた暗号化は非常に有効であるが、そのメディアでしか再生できないという欠点があったが、外部から操作不可能なメディア制御器内で、暗号化鍵情報とメディアID情報を管理し、コピーと同時に削除することで、ユーザーの使い勝手の良いシステムを提供することが出来るようになる。データ移動後のデータ

構造は図4(3)のようになる。移動終了後始めの64ビットのデータリンクID情報は、差分IDのデータ情報として書き換えられる。

【0029】次に、メディアBに移動された暗号化コンテンツ情報EG1(X1)を再生する場合を説明する。再生手順は、前記配信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報を再生する場合、メディアBをメディア制御器にセットし、メディア制御器を「再生モード」とする。暗号化鍵情報EA(G1)を自分のIDであるBに α を加算した値、即ち、 $B+(A-B)$ を用いて暗号化鍵G1を復号し、次に暗号化鍵G1を用いて暗号化コンテンツ情報EG1(X1)を復号して再生データX1を得ることが出来る。差分IDである $\alpha=A-B$ なのでID=Aを用いて復号したのと等価であり、再生が可能となる。

【0030】次に、コンテンツの記録されている譲渡元メディアAからバックアップ用メディアに暗号化コンテンツ情報をコピーする場合について説明する。バックアップメディアとは、メディア制御器に着脱できないメディアを総称して言う。即ちPCのハードディスクや、記録可能な光ディスクなど、本方式の制御器を有していない場合がこれに当たる。ここでは端末PCに接続されたハードディスクをバックアップメディアとする。

【0031】まず、メディアAをメディア制御器にセットして、メディア制御器を「バックアップ出力モード」とする。メディア制御器をPC端末に接続する。暗号化鍵情報EA(G1)と譲渡元メディアAのIDはメディア制御器のメモリーにデータリンクIDによって対応づけられた形態で記録される。これは図3のメディア制御器内メモリーブロックに示したように、データリンクIDとしてDnという管理ナンバーを一つ選ぶ。このDnに関連して、暗号化鍵情報EA(G1)とメディアAのIDが記録される。暗号化コンテンツ情報EG1(X1)には上記データリンクIDが付加されてメディア制御器を介して暗号化鍵情報EA(G1)と共に端末PCに接続されたハードディスクに転送される。暗号化コンテンツ情報構造を図5に示す。

【0032】次に、コンテンツの記録されているバックアップ用メディアから譲渡先メディアBに暗号化コンテンツ情報をコピーする場合について説明する。まず、メディアBをメディア制御器にセットして、メディア制御器を「バックアップ入力モード」とする。メディア制御器をPC端末に接続する。バックアップ用メディアに記録されている暗号化コンテンツデータの先頭64ビットは必ずデータリンクDnである。上記データリンクIDが付加されている暗号化コンテンツ情報EG1(X1)と暗号化鍵情報EA(G1)を譲渡先メディアBにコピーする。

【0033】メディア制御器は、接続された譲渡先メディアのID(B)を読み取り、暗号化コンテンツ情報EG1(X1)に付加されたデータリンクIDを読み取り、暗号化鍵情報EA(G1)を読み取る。それをもとにメディア制御器

のメモリーからデータリンクIDに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのID (A) を読み取り、譲渡先メディアBから読み出した暗号化鍵情報EA(G1)と制御器メモリーから読み出した暗号化鍵情報EA(G1)とを照合する。

【0034】認証の結果一致している場合、譲渡先メディアBと譲渡元メディアAのIDの差分値である差分ID、

(A-B) 値を、譲渡先メディアBに記録する。そして記録後、メディア制御器のメモリーに記録されている前記暗号化鍵情報EA(G1)と譲渡元メディアのID (A) を消去する。このバックアップの動作は図3のメディアAからメディアBへデータを移動した場合と、メディアAから一旦バックアップ用メディアにバックアップし、その後メディアBへ移動したものと等価になる。

【0035】バックアップメディアからメディアBに移動された暗号化コンテンツ情報EG1(X1)を再生する場合は、すでに説明した前記配信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報EG1(X1)を再生する場合、メディアBをメディア制御器にセットし、メディア制御器を「データ再生モード」とする。暗号化鍵情報EA(T1D)を自分のIDであるBに α を加算した値、即ち、 $B + (A - B)$ を用いて暗号化鍵G1を復号し、次に暗号化鍵G1を用いて暗号化コンテンツ情報EG1(X)を復号して再生データXを得ることが出来る。差分IDの $\alpha = A - B$ なのでID=Aを用いて復号したのと等価であり、再生が可能となる。

【0036】ここでの方式は暗号化コンテンツ情報は公開鍵方式で暗号化されたこととして説明したが、端末の共通鍵Gでセンターから配信され、端末では復号鍵Gを用いても可能である。またメディア固有のIDにて、鍵を暗号化することとして説明したが、IDそのものではなく、所定の関数を用いてIDを変換した情報を用いた鍵で暗号化してもよい。

【0037】次に、図6を用いて本発明の実施例のブロック図について説明する。最初に配信センターからメディアAにコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器21にセットする。メディア制御器を端末T1にセットして、外部インターフェースよりメディア制御器のモード設定部51に「データ記録モード」を設定する。課金、認証など所定の手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵(コンテンツ鍵)G1で暗号化されて端末T1に配信されてくる。「データ記録モード」の場合、モード設定部51は差分ID発生部52に「0」を発生させるよう指示する。メディア制御器では暗号化コンテンツデータを受信し、暗号化コンテンツデータヘッダー書き込み部53で、64ビットの「0」を示すデータをヘッダーに書き込み、暗号化コンテンツ情報EG1(X1)をメディアAのメモリー部33に記録する。モード設定部51に「データ記録モード」と設定されているとき、スイッ

チ2は差分ID発生部52につながるように切り替えられている。

【0038】一方メディア側のメディアID発生部31により発生された信号は、メディア制御器のメディアID読み取り部54によってメディアのID (A) を検出し、このID (A) でコンテンツの暗号化鍵G1を、鍵暗号化部55で暗号化して暗号化鍵情報EA(G1)を作成し、メディアのメモリー情報記録消去制御部32を介してメモリー部33に記録する。ヘッダーは差分IDを示し、この時点では0が記録されている。配信直後のデータ構造を図4(1)に示す。データは先頭に差分ID64ビット、暗号化鍵情報64ビット、その後ろに暗号化コンテンツ情報が記録される。

【0039】次に、メディアAに記録されている暗号化コンテンツ情報EG1(X1)を再生する場合を説明する。メディアAをメディア制御器21にセットし、外部インターフェースよりメディア制御器のモード設定部51に「データ再生モード」を設定する。メディア制御器21はメディアAのメモリー部33から暗号化鍵情報EA(G1)を読み出し、暗号化鍵復号部56に送信する。またメディア側のメディアID発生部31により発生された信号は、メディア制御器のメディアID読み取り部54によってメディアのID (A) を検出し、暗号化復号部56に送信する。また、メディア制御器21はメディアのメモリー部33からメモリー情報記録消去制御部32を介して暗号化コンテンツ情報EG1(X1)を読み出し、暗号化コンテンツデータヘッダー読み取り部57に送信する。暗号化コンテンツデータヘッダー読み取り部57では、先頭にある差分データ64ビットを読み、スイッチ1を介して差分ID読み取り部58へ送信される。

【0040】モード設定部51によって「データ再生モード」の場合、スイッチ1は差分ID読み取り部58へ切り替えられている。差分ID読み取り部58で検出された差分IDは暗号化鍵復号部56に送信される。暗号化鍵復号部56では、入力された差分IDとメディアIDを加算し、IDを生成し、暗号化鍵G1を復号する。ここでは差分ID=0なのでID=Aを用いて復号したのと等価である。復号した暗号化鍵G1は暗号化コンテンツデータ復号部59に送信される。また、暗号化コンテンツデータヘッダー読み取り部57でヘッダーが取り去られた暗号化コンテンツデータは暗号化コンテンツ復号部59に送信される。暗号化コンテンツデータ復号部59では、入力された暗号化コンテンツデータEG1(X1)と暗号化鍵G1によって暗号化コンテンツデータを復号化し、再生データXとして出力する。

【0041】次に、メディアAからメディアBへデータを譲渡(移動)する場合を説明する。コンテンツの記録されている譲渡元メディアAから譲渡先メディアBに暗号化コンテンツ情報をコピーする場合、まず、メディア制御器21にメディアAをセットする。外部インターフェー

スよりメディア制御器のモード設定部 5 1 に「データ移動出力モード」を設定する。

【0042】メディアID発生部 3 1 により発生された信号は、メディア制御器のメディアID読み取り部 5 4 によってメディアのID (A) を検出し、メディア制御器内メモリー 6 0 の記録再生消去制御部 6 1 に送信される。同時に暗号化鍵情報 EA(G1) がメディア A から呼び出され、メディア制御器内メモリー 6 0 の記録再生消去制御部 6 1 に送信される。また、データリンクID発生部 6 2 でデータリンクIDが発生されてメディア制御器内メモリー 6 0 の記録再生消去制御部 6 1 に送信される。これら暗号化鍵情報 EA(G1) と譲渡元メディア A のID はメディア制御器のメモリー 6 0 にデータリンクIDによって対応づけられた形態で記録される。後述するような、データリンクIDを消去する場合には消去した情報がデータリンクID発生部に送信され、矛盾なく管理できるIDが発生できるようになっている。

【0043】データリンクID発生部 6 2 は同時に、暗号化コンテンツデータヘッダー書き込み部 5 3 にもデータリンクIDを送信する。モード設定部 5 1 に「データ移動出力モード」と設定されているとき、スイッチ 2 は、データリンクID発生部 6 2 につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部 5 3 では、メディア A のメモリー部 3 3 から暗号化コンテンツデータを読み取り、ヘッダーにデータリンクIDを書き込んで、一旦メディアのメモリー 3 3 に戻される。

【0044】戻された暗号化コンテンツデータは暗号化鍵情報とともにデータ移動用の領域に格納され、メディアバス 3 4 を介して、高速にメディア B に転送される。このメディアバス 3 4 は、メディア A とメディア B を物理的に連結して、メディア制御器を介さずにデータ転送を行う。このデータ自体は暗号化コンテンツデータのみがこのメディアバスを通過できるようになっているので安全性が高い。

【0045】その後、メディア側のメモリー情報記録消去制御部 3 2 は設定モードが「データ移動出力モード」であることを確認して、譲渡元メディア A にある暗号化鍵情報 EA(G1) を消去する。暗号化コンテンツ情報構造を図 4 (2) に示す。

【0046】次に、メディア制御器 2 1 にメディア B をセットする。メディア制御器のメディアID読み取り部 5 4 によってメディアのID (B) を検出する。そしてメディア B のメモリー部 3 2 B にすでに転送記録されている暗号化コンテンツ情報 EG1 (X1) を暗号化コンテンツデータヘッダー読み取り部 5 7 に送信する。また、メディア B に記録されている暗号化鍵情報 EA(G1) を読み取る。

【0047】モード設定部 5 1 に「データ入力移動モード」と設定されているとき、スイッチ 1 はデータリンクID読み取り部 6 3 につながるように切り替えられている。データリンクID読み取り部 6 3 では、暗号化コンテ

ンツ情報 EG1 (X1) のヘッダーについているデータリンクIDを読み取り、メディア制御器内メモリー 6 0 の記録再生消去制御部 6 1 に送信する。記録再生消去制御部 6 1 ではこのデータリンクIDをもとに、メディア制御器のメモリー 6 0 からデータリンクIDのDnに対応づけられた暗号化鍵情報 EA(G1) と譲渡元メディアのIDであるID(A)を読み取る。

【0048】ここで、譲渡先メディア B から読み出した暗号化鍵情報 EA(G1) とメディア制御器メモリー 6 0 から読み出した暗号化鍵情報 EA(G1) を暗号化鍵照合部 6 4 に送信し照合する。この鍵情報が一致していなければ以下のプロセスである差分IDを発行しない。照合結果は差分ID発生部 5 2 に送信され、照合結果が一致している場合、ID(A) は差分ID発生部 5 2 に送信される。差分ID発生部 5 2 では入力されたID(A) と、メディアID読み取り部 5 4 によって読み取った譲渡先メディアのID (B) との差を計算し、差分ID (A-B) 値を、暗号化コンテンツデータヘッダー書き込み部 5 3 に送信する。

【0049】モード設定部 5 1 に「データ入力移動モード」と設定されているとき、スイッチ 2 は差分ID発生部 5 2 につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部 5 3 は対象となるデータリンクIDのついた暗号化コンテンツデータのヘッダーを差分IDの値に書き換える。

【0050】その後、暗号化コンテンツデータヘッダー書き込み部 5 3 は、書き込み完了の信号をメディア制御器内メモリー 6 0 の記録再生消去制御部 6 1 に出し、記録再生消去制御部 6 1 は前記暗号化鍵情報 EA(G1) と譲渡元メディアのID (A) を消去する。データ移動後のデータ構造は図 4 (3) のようになる。移動終了後始めの 6 4 ビットのデータリンクID情報は、差分IDのデータ情報として書き換えられる。

【0051】次に、メディア B に移動された暗号化コンテンツ情報を再生する場合を説明する。再生手順は、前記配信後のメディア A を再生する手順と同じである。即ち、このメディア B に記録されている暗号化コンテンツ情報 EG1 (X1) を再生する場合、メディア B をメディア制御器 2 1 にセットし、メディア制御器を「データ再生モード」とする。メディア制御器 2 1 はメディア B のメモリー部 3 3 B から暗号化鍵情報 EA(G1) を読み出し、暗号化鍵復号部 5 6 に送信する。またメディア側のメディアID発生部 3 1 B により発生された信号は、メディア制御器のメディアID読み取り部 5 4 によってメディアのID (B) を検出し、暗号化復号部 5 6 に送信する。また、メディア制御器 2 1 はメディア B のメモリー部 3 3 B から暗号化コンテンツ情報 EG1 (X1) を読み出し、暗号化コンテンツデータヘッダー読み取り部 5 7 に送信する。暗号化コンテンツデータヘッダー読み取り部 5 7 では、先頭にある差分データ 6 4 ビットを読み、スイッチ 1 を介して差分ID読み取り部 5 8 へ送信される。

10

20

30

40

50

【0052】モード設定部51によって「データ再生モード」の場合、スイッチ1は差分ID読み取り部58へ切り替えられている。差分ID読み取り部58で検出された差分IDは暗号化鍵復号部56に送信される。暗号化鍵復号部56では、入力された差分IDとメディアIDを加算し、IDを生成し、暗号化鍵G1を復号する。ここでは差分ID=A+BとなっていてID=B+(A-B)、即ちID=Aを用いて復号したのと等価である。復号した暗号化鍵G1は暗号化コンテンツデータ復号部59に送信される。また、暗号化コンテンツデータヘッダー読み取り部57でヘッダー

が取り去られた暗号化コンテンツデータEG1(X1)は暗号化コンテンツ復号部59に送信される。暗号化コンテンツデータ復号部59では、入力された暗号化コンテンツデータを復号化し、再生データとして出力する。

【0053】次に、コンテンツの記録されている譲渡元メディアAからバックアップ用メディア70に暗号化コンテンツ情報をコピーする場合について説明する。まず、メディア制御器21にメディアAをセットする。外部インターフェースよりメディア制御器のモード設定部

51に「バックアップ出力モード」を設定する。メディア制御器21を端末T1に接続する。端末T1をバックアップ用メディア70に接続する。

【0054】メディアID発生部31により発生された信号は、メディア制御器のメディアID読み取り部54によってメディアAのID(A)を検出し、メディア制御器内メモリー60の記録再生消去制御部61に送信される。同時に暗号化鍵情報がメディアAから呼び出され、メディア制御器内メモリー60の記録再生消去制御部61に送信される。

【0055】また、データリンクID発生部62でデータリンクIDが発生されてメディア制御器内メモリー60の記録再生消去制御部61に送信される。これら暗号化鍵情報EA(G1)と譲渡元メディアAのIDはメディア制御器のメモリー60にデータリンクIDによって対応づけられた形態で記録される。データリンクID発生部62は同時に、暗号化コンテンツデータヘッダー書き込み部53にもデータリンクIDを送信する。モード設定部51に「バックアップ出力モード」と設定されているとき、スイッチ2は、データリンクID発生部62につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部53では、メディアAのメモリー部33から暗号化コンテンツデータを読み取り、ヘッダーにデータリンクIDを書き込む。データリンクIDが書き込まれた暗号化コンテンツデータEG1(X1)は、メディアAのメモリー部33から読み出された暗号化鍵情報EA(G1)と共に、端末T1を介してバックアップメディア70に送信される。暗号化コンテンツ情報構造を図4(2)に示す。その後、譲渡元メディアAにある暗号化鍵情報EA(G1)はメモリー情報記録消去制御部32によって消去される。

【0056】次に、コンテンツの記録されているバックアップ用メディア70から譲渡先メディアBに暗号化コンテンツ情報を譲渡する場合について説明する。まず、メディアBをメディア制御器21にセットして、メディア制御器21を「バックアップ入力モード」とする。メディア制御器のメディアID読み取り部54によってメディアのID(B)を検出する。次に、アップメディア70から端末T1を介して暗号化コンテンツデータEG1(X1)と暗号化鍵情報EA(G1)を読み出し、その暗号化コンテンツデータEG1(X1)と暗号化鍵情報EA(G1)を暗号化コンテンツデータヘッダー書き込み部53を通過させて、メディアBのメモリー部33Bに記録させる。

【0057】続いて、暗号化コンテンツ情報EG1(X1)をメディアBのメモリー部33Bから暗号化コンテンツデータヘッダー読み取り部57に送信する。モード設定部51に「バックアップ入力モード」と設定されているとき、スイッチ1はデータリンクID読み取り部63につながるように切り替えられている。データリンクID読み取り部63では、暗号化コンテンツ情報EG1(X1)のヘッダーについているデータリンクIDを読み取り、メディア制御器内メモリー60の記録再生消去制御部61に送信する。また、メディアBのメモリー部33Bから暗号化鍵情報EA(G1)も読み取る。記録再生消去制御部61ではこのデータリンクIDをもとに、メディア制御器のメモリーからデータリンクIDのDnに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのIDであるID(A)を読み取る。

【0058】ここで、譲渡先メディアBから読み出したEA(G1)と制御器メモリー60から読み出したEA(G1)を暗号化鍵照合部64に送信し照合する。この鍵情報が一致していなければ以下のプロセスである差分IDを発行しない。照合結果は差分ID発生部52に送信され、照合結果が一致している場合、ID(A)は差分ID発生部に送信される。

【0059】差分ID発生部52では入力されたID(A)と、メディアID読み取り部54によって読み取った譲渡先メディアのID(B)との差を計算し、差分ID(A-B)値を、暗号化コンテンツデータヘッダー書き込み部53に送信する。モード設定部51に「バックアップ入力モード」と設定されているとき、スイッチ2は差分ID発生部52につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部53は対象となるデータリンクIDのついた暗号化コンテンツデータEG1(X1)のヘッダーを差分IDの値に書き換える。その後、暗号化コンテンツデータヘッダー書き込み部53は、書き込み完了の信号をメディア制御器内メモリー60の記録再生消去制御部61に出力し、記録再生消去制御部61は前記暗号化鍵情報EA(G1)と譲渡元メディアのID(A)を消去する。

【0060】データ移動後のデータ構造は図4(3)の

ようになる。移動終了後始めの 64 ビットのデータリンク ID 情報は、差分 ID のデータ情報として書き換えられる。

【0061】次に、バックアップメディア 70 からメディア B に移動された暗号化コンテンツ情報を再生する場合を説明する。再生手順は、前記配信後のメディア A を再生する手順と同じである。即ち、このメディア B に記録されている暗号化コンテンツ情報 E G1 (X1) を再生する場合、メディア B をメディア制御器 21 にセットし、メディア制御器を「データ再生モード」とする。

【0062】メディア制御器 21 はメディア B のメモリー部 33 B から暗号化鍵情報 E A (G1) を読み出し、暗号化鍵復号部 56 に送信する。また、メディア側のメディア ID 発生部 31 B により発生された信号は、メディア制御器のメディア ID 読み取り部 54 によってメディアの ID (B) を検出し、暗号化鍵復号部 56 に送信する。また、メディア制御器はメディア B のメモリー部 33 B から暗号化コンテンツ情報 E G1 (X1) を読み出し、暗号化コンテンツデータヘッダー読み取り部 57 に送信する。暗号化コンテンツデータヘッダー読み取り部 57 では、先頭にある差分データ 64 ビットを読み、スイッチ 1 を介して差分 ID 読み取り部 58 へ送信される。

【0063】モード設定部 51 によって「データ再生モード」の場合、スイッチ 1 は差分 ID 読み取り部 58 へ切り替えられている。差分 ID 読み取り部 58 で検出された差分 ID は暗号化鍵復号部 56 に送信される。暗号化鍵復号部 56 では、入力された差分 ID とメディア ID を加算し、ID を生成し、暗号化鍵 G1 を復号する。ここでは差分 ID = A - B となっていて ID = B + (A - B)、即ち ID = A を用いて復号した場合と等価である。復号した暗号化鍵 G1 は暗号化コンテンツデータ復号部 59 に送信される。また、暗号化コンテンツヘッダー読み取り部 57 でヘッダーが取り去られた暗号化コンテンツデータ E G1 (X1) は暗号化コンテンツデータ復号部 59 に送信される。暗号化コンテンツデータ復号部 59 では、入力された暗号化コンテンツデータ E G1 (X1) と暗号化鍵 G1 によって暗号化コンテンツデータを復号化し、再生データ X1 として出力する。

【0064】このように、本実施例によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。

【0065】また、本実施例によれば、1 人のユーザーが複数のメディアを持っていた場合、不正なコピーを防止しつつ、そのメディア間でデータの移動や、一時バックアップをしてから、任意のメディアにデータを復帰させるシステムを提供できる。

【0066】さらに、メディアが着脱可能なメディア制御器を有し、メディア制御器にはメモリーを有し、メデ

ディア間の暗号化コンテンツ情報 E G1 (X1) の移動を行う場合には、暗号化鍵情報 E A (G1) をメモリーに一時記録して移動終了後暗号化鍵情報 E A (G1) を消去し、バックアップ用メディアに移動する場合には、次にバックアップ用メディアから復帰するまで暗号化鍵情報 E A (G1) をメモリーに一時記録して復帰時に暗号化鍵情報 E A (G1) を消去するようにしたので、一時バックアップをしてから、任意のメディアにデータを復帰させる時などに、不正な複製メディアへのコピーを防止しつつ、メディア間のデータ移動を自由に行うことが可能となる。

【0067】また、メディア制御器内メモリーに一時記録した移動元メディアの暗号化鍵情報 E A (G1) と、移動先のメディア内から読み出した移動元メディアの暗号化鍵情報 E A (G1) とが同一か否かを認証し、同一と認証したときのみ差分 ID を生成し記録するようにしたので、同一のメディア A から複数のメディア制御器を使って、データ移動を行った場合に発生する問題を回避できる。さらには、この認証機能は、不正にコピーしようとしてメディア制御器内メモリーのデータや、メディア内データを改ざんしようとした場合に発生する矛盾を発見し、機能を停止するのに効果を発揮する。

【0068】

【発明の効果】本発明によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。

【0069】また、本発明によれば、1 人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメディアにデータを復帰させるシステムを提供できる。

【図面の簡単な説明】

【図 1】一実施例に用いるデータ配信時の暗号化を説明するための図である。

【図 2】一実施例の構成を示す図である。

【図 3】一実施例の機能説明図である。

【図 4】一実施例のメディア内のデータ構造図である。

【図 5】一実施例のバックアップ用メディア内のデータ構造図である。

【図 6】一実施例の詳細構成を示すブロック図である。

【符号の説明】

21 メディア制御器 (コンテンツ情報処理装置、コンテンツ情報復元装置)

52 差分 ID 発生部 (独自 ID 情報形成手段)

53 暗号化コンテンツデータヘッダー書き込み部 (データリンク ID 書き込み手段)

56 暗号化鍵復号部 (コンテンツ鍵復元手段)

59 暗号化コンテンツデータ復号部 (コンテンツ情報復元手段)

10

20

30

40

50

60 メディア制御器内メモリ（第1のメディアのメディアIDに関する情報を一時記録するメモリ）
 61 記録再生消去制御部（消去手段、メモリ読み出し

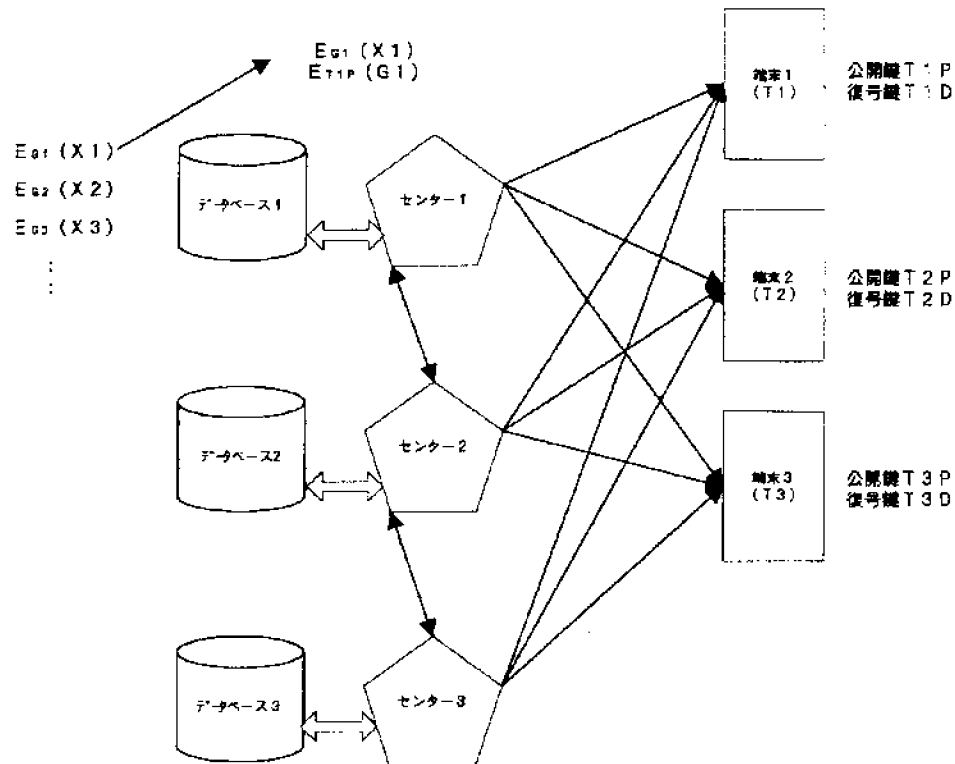
手段）

64 暗号化鍵認証部（暗号化鍵情報照合手段）

70 バックアップ用メディア

【図1】

図1



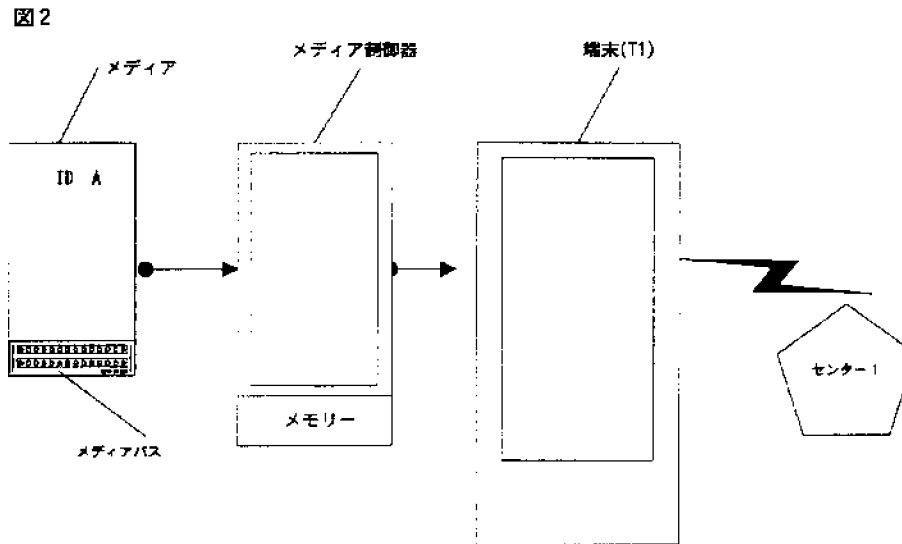
【図4】

図4

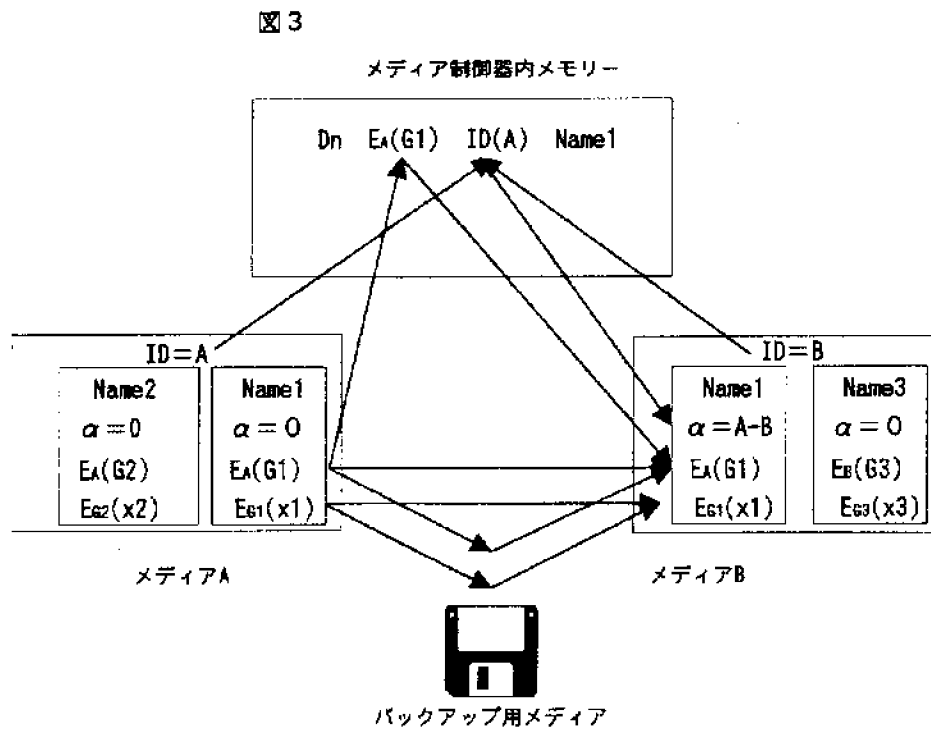
メディア内データ構造

| 差分ID/データリンクID | 暗号化鍵情報E _k (G1) | 暗号化コンテンツ情報E _c (X1) |
|----------------|---------------------------|---|
| 64ビット | 64ビット | |
| (1) 配信されたデータ構造 | 0 | 暗号化鍵情報E _k (G1) 暗号化コンテンツ情報E _c (X1) |
| (2) 移動途中のデータ構造 | Dn | 暗号化鍵情報E _k (G1) 暗号化コンテンツ情報E _c (X1) |
| (3) 移動後のデータ構造 | A-B | 暗号化鍵情報E _k (G1) 暗号化コンテンツ情報E _c (X1) |

【図 2】



【図 3】



【図 5】

図 5

バックアップ用メディア内データ構造

| データリンクID | 暗号化鍵情報E _k (G1) | 暗号化コンテンツ情報E _s (X1) |
|----------|---------------------------|-------------------------------|
| 64ビット | 64ビット | |

Aからバックアップ
メディアにヘ
コピー後のデー
タ構造

| D _n | 暗号化鍵情報E _k (G1) | 暗号化コンテンツ情報E _s (X1) |
|----------------|---------------------------|-------------------------------|
|----------------|---------------------------|-------------------------------|

【図 6】

